

What is claimed is:

1 1. A system for encrypting a portion of token data, for recording said token
2 data with a portion of said token data in an encrypted form on a computer
3 readable medium, and for reading said token data and decrypting said portion of
4 said token data, wherein

5 said system comprises a plurality of client computers and a server,
6 said server generates a secure transfer key pair and encrypts a private
7 key of said secure transfer key pair,

8 said secure transfer key pair is transferred to each of said client
9 computers in said plurality thereof with said private key of said secure transfer
10 key pair in an encrypted form,

11 each client computer in said plurality thereof is programmed to generate
12 token data including said portion of said token data encrypted with a public key of
13 said secure transfer key pair, to record said token data on a computer readable
14 medium, to read said token data from said computer readable medium, to
15 decrypt said private key of said secure transfer key pair, and to decrypt said
16 portion of said token data with said private key of said secure transfer key pair.

1 2. The system of claim 1, wherein

2 each client computer in said plurality thereof generates a platform key
3 pair,

4 a public key of said platform key pair is transferred to said server,

5 said secure transfer key pair is transferred to each of said client
6 computers in said plurality thereof with said private key of said secure transfer
7 key pair encrypted with said public key of said platform key pair of said client
8 computer, and each client computer in said plurality thereof stores said secure
9 transfer key pair with said private key of said secure transfer key pair encrypted

1 with said public key of said platform key pair and subsequently decrypts said
2 private key of said secure transfer key pair with said private key of said platform
3 key pair.

1 3. The system of claim 2, wherein
2 each client computer in said plurality thereof includes a security
3 subsystem having a subsystem processor and subsystem storage,
4 each client computer in said plurality thereof generates a hardware key
5 pair within said security subsystem
6 a private key of said hardware key pair is stored in said subsystem
7 storage, and
8 a private key of said platform key pair is encrypted with said hardware
9 public key and is decrypted with said hardware private key in said security
10 subsystem before said private key of said platform key pair is used to decrypt
11 said private key of said secure transfer key pair within said security subsystem.

1 4. The system of claim 1, wherein each client computer within said plurality
2 of client computers is enabled to perform a predetermined task in response to
3 decrypting said portion of said token data.

1 5. The system of claim 1, wherein
2 each client computer in said plurality of client computers includes an input
3 device for providing a numeric input,
4 said portion of said token data includes a PIN,
5 each client computer in said plurality of client computers, after decrypting
6 said portion of said token data read from said computer readable medium,
7 compares said PIN included within said token data with said numeric input
8 provided through said input device, and

5 each of said client computers in said plurality thereof reads said secure
6 transfer key pair with said private key of said secure transfer key pair in said
7 encrypted form from said computer readable medium.

1 9. The system of claim 8, wherein

2 each client computer in said plurality thereof generates a platform key pair
3 and writes a public key of said platform key pair on a first computer readable
4 medium,

5 said server reads said public key of said platform key pair from each client
6 computer in said plurality thereof , encrypts said private key of said secure
7 transfer key pair with said public key of said platform key pair, and writes said
8 secure transfer key pair on a second computer readable medium with said
9 private key of said secure transfer key pair encrypted with said public key of said
10 client computer,

11 said client computer reads said secure transfer key pair with said private
12 key so said secure transfer key pair encrypted with said public key of said client
13 computer from said second computer readable medium, stores said secure
14 transfer key pair with said private key of said secure transfer key pair encrypted
15 with said public key of said platform key pair and subsequently decrypts said
16 private key of said secure transfer key pair with said private key of said platform
17 key pair.

1 10. A method within a computing system for encrypting token data, for
2 recording said token data in an encrypted form on a computer readable medium,
3 and for reading and decrypting token data recorded on a computer readable
4 medium, wherein said method comprises:
5 receiving a secure transfer key pair ;
6 storing said secure transfer key pair;

7 after storing said secure transfer key pair, in response to an indication that token
 8 data is to be recorded, encrypting a portion of said token data with a public key of
 9 said secure transfer key pair; and recording said token data, including said
 10 portion of said token data encrypted with said public key of said secure transfer
 11 key pair on a computer readable medium; and
 12 after storing said secure transfer key pair, in response to an indication that token
 13 data is to be read, reading said token data from a computer readable medium,
 14 and decrypting a portion of said data with a private key of said secure transfer
 15 key pair.

1 11. The method of claim 10, wherein said secure transfer key pair is received
 2 from said server over a communications network.

1 12. The method of claim 11, additionally comprising:
 2 generating and storing a platform key pair;
 3 transmitting a public key of said platform key pair to said server over said
 4 communications network, wherein said secure transfer key pair is subsequently
 5 received from said server encrypted with said public key of said platform key pair,
 6 and wherein said private key of said secure transfer key pair is stored encrypted
 7 with said public key of said platform key pair, and
 8 decrypting said private key of said secure transfer key pair with said
 9 private key of said platform key pair before decrypting said portion of said data
 10 with said private key of said secure transfer key pair.

1 13. The method of claim 10, wherein said secure transfer key pair is read from
 2 a computer readable medium.

14. The method of claim 13, additionally comprising:
generating and storing a platform key pair; writing a public key of said platform key pair on a computer readable medium,
reading said secure transfer key pair from a computer readable medium encrypted with said public key of said platform key pair, and wherein said private key of said secure transfer key pair is stored encrypted with said public key of said platform key pair, and
decrypting said private key of said secure transfer key pair with said private key of said platform key pair before decrypting said portion of said data with said private key of said secure transfer key pair.

15. The method of claim 10, additionally comprising:
generating and storing a hardware key pair within a security subsystem of said computing system, wherein a private key of said hardware key pair is stored within said security subsystem of said computing system;
encrypting said private key of said platform key pair with said public key of said hardware key pair, wherein said platform key pair is stored with said private key of said platform key pair encrypted with said public key of said hardware key pair; and
decrypting said private key of said platform key pair with said private key of said hardware key pair within said security subsystem before decrypting said private key of said secure transfer key pair with said private key of said platform key pair.

16. The method of claim 10, additionally comprising enabling performance of a predetermined task in response to decrypting said portion of said data with said private key of said secure transfer key pair.

1 17. The method of claim 10, wherein
 2 said portion of said token data includes a PIN, and
 3 said method additionally comprises receiving a numeric input from an
 4 input device, comparing said PIN with said numeric input from said input device,
 5 and enabling performance of a predetermined task in response to determining an
 6 equivalence between said PIN and said numeric input.

1 18. A computer readable medium having recorded thereon computer
 2 executable instructions for performing a method within a computing system for
 3 encrypting token data, for recording said token data in an encrypted form on a
 4 computer readable medium, and for reading and decrypting token data recorded
 5 on a computer readable medium, wherein said method comprises:
 6 receiving a secure transfer key pair from said server; storing said secure
 7 transfer key pair;
 8 after storing said secure transfer key pair, in response to an indication that
 9 token data is to be recorded, encrypting a portion of said token data with a public
 10 key of said secure transfer key pair; and recording said token data, including said
 11 portion of said token data encrypted with said public key of said secure transfer
 12 key pair on a computer readable medium; and
 13 after storing said secure transfer key pair, in response to an indication that
 14 token data is to be read, reading said token data from a computer readable
 15 medium, and decrypting a portion of said data with a private key of said secure
 16 transfer key pair.

1 19. The computer readable medium of claim 18, wherein said secure transfer
 2 key pair is received from said server over a communications network.

1 20. The computer readable medium of claim 19, wherein said method
2 additionally comprises:

3 generating and storing a platform key pair;
4 transmitting a public key of said platform key pair to said server over said
5 communications network, wherein said secure transfer key pair is subsequently
6 received from said server encrypted with said public key of said platform key pair,
7 and wherein said private key of said secure transfer key pair is stored encrypted
8 with said public key of said platform key pair, and
9 decrypting said private key of said secure transfer key pair with said
10 private key of said platform key pair before decrypting said portion of said data
11 with said private key of said secure transfer key pair.

1 21. The computer readable medium of claim 18, wherein said secure transfer
2 key pair is read from a computer readable medium.

1 22. The computer readable medium of claim 21, wherein said method
2 additionally comprises:

3 generating and storing a platform key pair;
4 writing a public key of said platform key pair on a computer readable
5 medium,
6 reading said secure transfer key pair from a computer readable medium
7 encrypted with said public key of said platform key pair, and wherein said private
8 key of said secure transfer key pair is stored encrypted with said public key of
9 said platform key pair, and
10 decrypting said private key of said secure transfer key pair with said
11 private key of said platform key pair before decrypting said portion of said data
12 with said private key of said secure transfer key pair.

23. The computer readable medium of claim 18, wherein said method additionally comprises:

generating and storing a hardware key pair within a security subsystem of said computing system, wherein a private key of said hardware key pair is stored within said security subsystem of said computing system; encrypting said private key of said platform key pair with said public key of said hardware key pair, wherein said platform key pair is stored with said private key of said platform key pair encrypted with said public key of said hardware key pair; and

decrypting said private key of said platform key pair with said private key of said hardware key pair within said security subsystem before decrypting said private key of said secure transfer key pair with said private key of said platform key pair.

24. The computer readable medium of claim 18, wherein said method additionally comprises enabling performance of a predetermined task in response to decrypting said portion of said data with said private key of said secure transfer key pair.

25. The computer readable medium of claim 18, wherein:

said portion of said token data includes a PIN, and

said method additionally comprises receiving a numeric input from an input device, comparing said PIN with said numeric input from said input device, and enabling performance of a predetermined task in response to determining an equivalence between said PIN and said numeric input.

26. A process of providing electrical signals over a communications network causing computer storage to have stored therein computer executable instructions for performing a method within a computing system for encrypting

32. The process of claim 26, wherein said method additionally comprises enabling performance of a predetermined task in response to decrypting said portion of said data with said private key of said secure transfer key pair.

33. The process of claim 26, wherein:
said portion of said token data includes a PIN, and
said method additionally comprises receiving a numeric input from an input device, comparing said PIN with said numeric input from said input device, and enabling performance of a predetermined task in response to determining an equivalence between said PIN and said numeric input.

34. A method for enabling performance of a predetermined task in a remote computer system through use of an encrypted portion of token data recorded in a local computer, wherein said method comprises:
transferring a secure transfer key pair from said server to said local computer;
storing said secure transfer key pair within said local computer;
establishing communication between said remote computer and said server;
transferring said secure transfer key pair from said server to said remote computer;
storing said secure transfer key pair within said remote computer;
encrypting said portion of said token data within said local computer with a public key of said secure transfer key pair;
recording said token data, including said portion of said token data encrypted with said public key of said secure transfer key pair, within said local computer on a computer readable medium;

transporting said computer readable medium from said local computer to said remote computer; reading said token data, including said portion of said token data encrypted with said public key of said secure transfer key pair, within said remote computer from a computer readable medium;

decrypting said portion of said token data within said remote computer with a private key of said secure transfer key pair; and

enabling said performance of said predetermined task in said remote computer in response to said portion of said token data.

35. The method of claim 18, wherein said secure transfer key pair is received from said server over a communications network.

36. The method of claim 34, additionally comprising:

generating and storing a first platform key pair within said local computer; and

transmitting a public key of said first platform key pair to said server from said local computer, wherein said secure transfer key pair is subsequently received by said local computer from said server encrypted with said public key of said first platform key pair, and wherein said private key of said secure transfer key pair is stored within said local computer encrypted with said public key of said first platform key pair.

37. The method of claim 34, wherein said secure transfer key pair is read from a computer readable medium.

1 38. The method of claim 37, wherein said method additionally comprises:
 2 generating and storing a platform key pair;
 3 writing a public key of said platform key pair on a computer readable
 4 medium,
 5 reading said secure transfer key pair from a computer readable medium
 6 encrypted with said public key of said platform key pair, and wherein said private
 7 key of said secure transfer key pair is stored encrypted with said public key of
 8 said platform key pair, and
 9 decrypting said private key of said secure transfer key pair with said
 10 private key of said platform key pair before decrypting said portion of said data
 11 with said private key of said secure transfer key pair.

1 39. The method of claim 34, additionally comprising:
 2 generating and storing a first hardware key pair in a security subsystem of
 3 said local computer, wherein a private key of said hardware key pair is stored
 4 within said security subsystem of said local computer;
 5 encrypting said private key of said first platform key pair with said public
 6 key of said first hardware key pair within said local computer, wherein said first
 7 platform key pair is stored within said local computer with said private key of said
 8 first platform key pair encrypted with said public key of said first hardware key
 9 pair.

1 40. The method of claim 34, additionally comprising:

2 generating and storing a second platform key pair within said remote
3 computer;

4 transmitting a public key of said second platform key pair to said server
5 from said remote computer, wherein said secure transfer key pair is
6 subsequently received by said remote computer from said server encrypted with
7 said public key of said second platform key pair, and wherein said private key of
8 said secure transfer key pair is stored within said remote computer encrypted
9 with said public key of said second platform key pair, and

10 decrypting said private key of said secure transfer key pair with said
11 private key of said second platform key pair within said remote computer before
12 decrypting said portion of said data with said private key of said secure transfer
13 key pair.

1 41. The method of claim 34, additionally comprising:

2 generating and storing a second hardware key pair within a security
3 subsystem of said remote computer, wherein a private key of said hardware key
4 pair is stored within said security subsystem of said remote computer;

5 encrypting said private key of said second platform key pair with said
6 public key of said second hardware key pair within said remote computer,
7 wherein said second platform key pair is stored within said remote computer with
8 said private key of said second platform key pair encrypted with said public key
9 of said second hardware key pair; and

10 decrypting said private key of said second platform key pair with said
11 private key of said second hardware key pair within said security subsystem of
12 said remote computer before decrypting said private key of said secure transfer
13 key pair with said private key of said second platform key pair.

42. The method of claim 36, additionally comprising enabling performance of a predetermined task within said remote computer in response to decrypting said portion of said data with said private key of said secure transfer key pair.

43. The method of claim 36, wherein
 said portion of said token data encrypted with said public key of said secure transfer key pair includes a PIN, and
 said method additionally comprises receiving a numeric input within said remote computer from an input device, comparing said PIN with said numeric input from said input device, and enabling performance of a predetermined task within said remote computer in response to determining an equivalence between said PIN and said numeric input.

44. A method for establishing a plurality of associated client computers, wherein a client computer in said plurality of associated client computers performs a predetermined task in response to reading and decrypting token data recorded on a computer readable medium, wherein said method comprises:
 generating a secure transfer key pair within a server;
 transferring said secure transfer key pair from said server to each client computer in said plurality of associated client computers;
 storing said secure transfer key pair within each client computer in said plurality of associated client computers;
 encrypting a first portion of token data with a public key of said secure transfer key pair within a first client computer within said plurality of associated client computers;
 recording token data on a computer readable medium, wherein said token data includes said first portion of token data encrypted with said public key of said secure transfer key pair, in said first client computer;

48. The method of claim 45, additionally comprising:

generating and storing a hardware key pair within a security subsystem of said client system, wherein a private key of said hardware key pair is stored within said security subsystem of said client computer;

encrypting said private key of said platform key pair with said public key of said hardware key pair, wherein said platform key pair is stored with said private key of said platform key pair encrypted with said public key of said hardware key pair; and

decrypting said private key of said platform key pair with said private key of said hardware key pair within said security subsystem before decrypting said private key of said secure transfer key pair with said private key of said platform key pair.

49. The method of claim 10, wherein

a portion of said token data includes a PIN, and said method additionally comprises receiving a numeric input from an input device, comparing said PIN with said numeric input from said input device, and enabling performance of a predetermined task in response to determining an equivalence between said PIN and said numeric input.

50. A method for establishing a plurality of associated client computers, wherein a client computer in said plurality of associated client computers performs a predetermined task in response to reading and decrypting token data recorded on a computer readable medium, wherein said method comprises:

generating a secure transfer key pair within a server; transferring said secure transfer key pair from said server to each client computer in said plurality of associated client computers; and

8 storing said secure transfer key pair within each client computer in said
9 plurality of associated client computers.

1 51. The method of claim 50, wherein
2 said method additionally comprises receiving a platform key pair from said
3 client computer within said plurality of associated client computers before
4 transferring said secure transfer key pair to said client computer,
5 said secure transfer key pair is transferred from said server to said client
6 computer with a private key of said secure transfer key pair encrypted with said
7 public key of said platform key pair.

1 52. The method of claim 51, wherein said secure transfer key pair is
2 transferred from said server to said client computer over a communications
3 network.

1 53. The method of claim 51, wherein said secure transfer key pair is
2 transferred from said server to said client computer as data recorded on a
3 computer readable medium.